(12) UK Patent Application (19) GB (11) 2 356 530 (13) A

(43) Date of A Publication 23.05.2001

(21) Application No 9927334.4

(22) Date of Filing 18.11.1999

(51) INT CL[7]
H04Q 7/38

(52) UK CL (Edition S)
H4L LRCMA L1H10 L213

(56) Documents Cited
GB 2279541 A WO 92/02087 A1 US 6014558 A
US 5471532 A US 4897875 A

(58) Field of Search
UK CL (Edition R) H4L LDSKA LDSKF LDSKX LEF
INT CL[7] H04Q 7/32 7/38
ONLINE: WPI, EPODOC, JAPIO

(71) Applicant(s)
Vodafone Limited
(Incorporated in the United Kingdom)
The Courtyard, 2-4 London Road, NEWBURY, Berkshire, RG14 1JX, United Kingdom

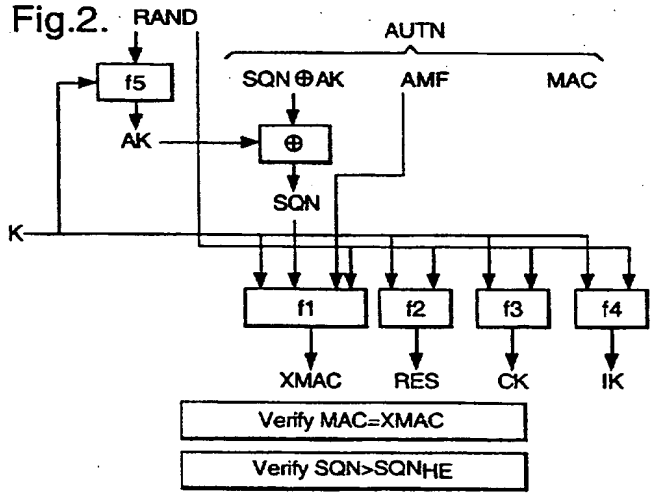
(72) Inventor(s)
Timothy James Wright

(74) Agent and/or Address for Service
Mathisen Macara & Co
The Coach House, 6-8 Swakeleys Road, Ickenham, UXBRIDGE, Middlesex, UB10 8BZ, United Kingdom

(54) Abstract Title
Mobile authentication using authentication vector

(57) Method and apparatus for authenticating a mobile user equipment in a mobile telecommunications network, where preferably the network is not the home operator network to which the equipment is directly subscribed. The aim of the invention is to directly provide the mobile user equipment with information to allow it to determine whether an authentication vector (AV) may be used for only one call or may be used for a predetermined period, which avoids the need to instruct the serving network on how to use the authentication vector. The mobile user equipment receives from a serving network at least an element of an authentication vector, where preferably the authentication vector is generated in the home operator network and includes an authentication management field (AMF). As claimed, the mobile may either extract the authentication management field from the received element and in response to at least a predetermined value of the management field, generate a predetermined key set identifier (KSI) to pass to the serving network with a call request, or decide, based at least in part on a value of a predetermined field contained in the received element, when to generate a termination message that is passed to the serving network to indicate that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls. Preferably the predetermined field is the authentication management field and the termination message a predetermined key set identifier. The decision as to when to generate the termination message may be based on the total call duration, the time elapsed or the total number of calls made since the authentication element was received.

Fig.2.



GB 2 356 530 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig.1.

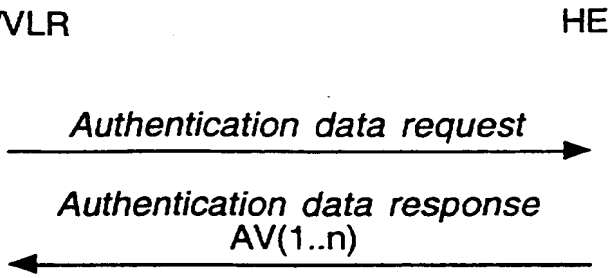


Fig.2.

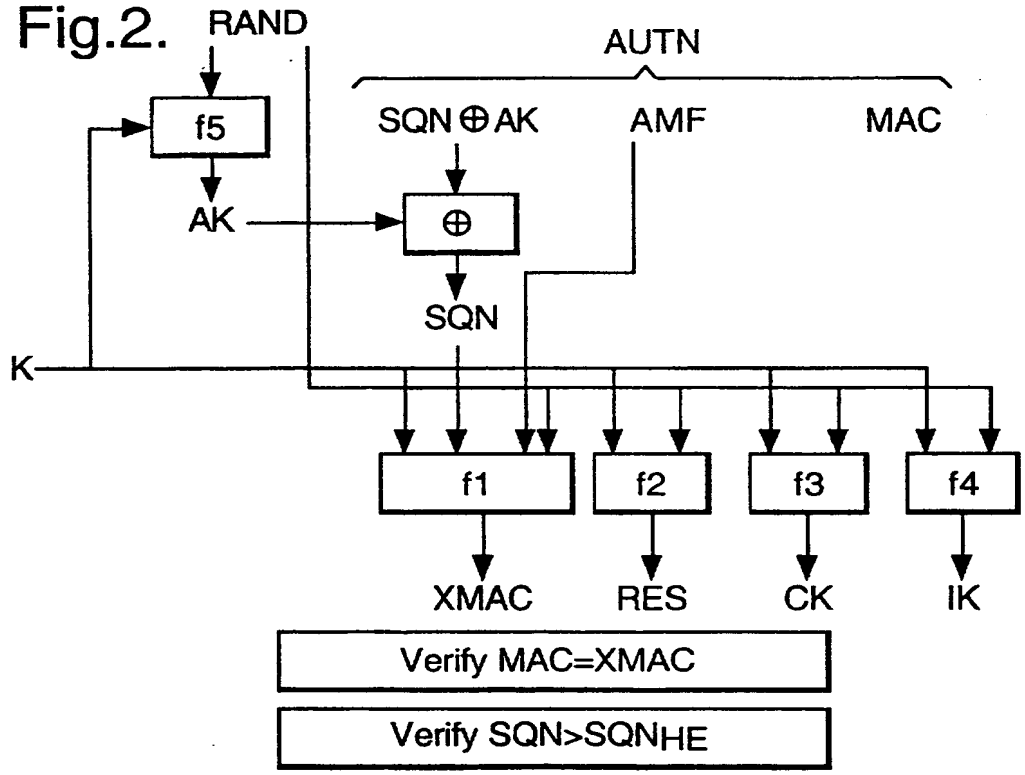
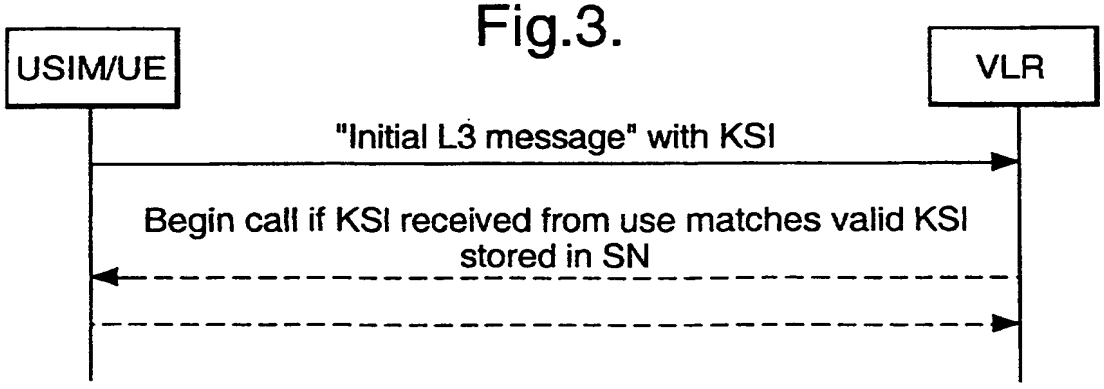


Fig.3.



USER AUTHENTICATION IN A MOBILE COMMUNICATIONS NETWORK

This invention relates to a method and apparatus for authenticating mobile user equipment in a mobile telecommunications network.

In accordance with a first aspect of the invention, there is provided a method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of passing an authentication element forming at least part of an authentication vector, from a serving network to mobile user equipment, deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

In accordance with a second aspect of the invention, there is provided a method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of requesting service from a serving network to which the user equipment is not directly subscribed, passing the request for service from the serving network to a home operator network to which the user equipment is directly subscribed, generating an authentication vector in the home operator network which includes an authentication management field, passing the authentication vector from the home operator network to the

serving network, passing an authentication element forming at least part of the authentication vector from the serving network to the user equipment, extracting in the user equipment an authentication management field from the authentication element, generating in response at least to a predetermined value of the authentication management field, a predetermined key set identifier, and passing the key set identifier to the serving network.

In accordance with a third aspect of the invention, there is provided mobile user equipment for use in a mobile telecommunications network including means for receiving from a serving network, an authentication element forming at least part of an authentication vector, decision means for deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and means for passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

Embodiments of networks and mobile user equipment in accordance with the invention will now be described by way of example with reference to the drawings in which:

Figure 1 is a schematic diagram of the flow of authentication information between a serving network and a home environment;

Figure 2 is a schematic block diagram of the processing of an authentication vector by mobile user equipment; and

Figure 3 is a schematic block diagram showing the flow of key set identification information between a mobile user and the visitor location register of a serving network.

The invention described below permits a 3GPP operator to use the 3GPP authentication management field AMF to direct a subscriber of that operator to ensure that a particular 3GPP authentication vector for that subscriber (from that operator) is used for only one call in a particular serving network. Alternatively the authentication vector may be used only for a predetermined time period, for a predetermined number of calls or for a predetermined total call duration (which may span more than one call) after issuance by the operator or receipt by the user equipment. The invention is applicable, for example, to 3GPP, 3GPP2, and IS-136 networks and to ANSI-41 networks which adopt the TR45 Enhanced Subscriber Authentication (ESA).

One possibility which has been considered is for a serving network (i.e. the network that a user is making calls with) to be given instructions on how the authentication vector should be used. However, this would require the home operator or home environment (i.e. the operator with which the user has a subscription) to rely on the competence of the serving network to ensure that the instructions are correctly followed. Furthermore, assuming that the instructions are passed electronically, new signalling messages would

need to be standardised and new procedures in the serving network visitor location registers (VLR's) would need to be devised, standardised and implemented to ensure that the VLR's respond correctly to the new signalling messages.

With reference to Figure 1, an authentication vector is transmitted from the home operator HE to the serving network SN in response to a so called "authentication data request" from the serving network.

An authentication vector contains the following parameters

RAND which is a random challenge generated by the home operator,

XRES which is the expected user response to RAND which is pre-computed by the home operator,

CK which is a cipher key,

IK which is an integrity key, and

a network user authentication string AUTN.

The network to user authentication string AUTN consists of

the sequence number for the vector (SQN) which is concealed with an anonymity key (AK),

an authentication management field AMF (discussed in detail below), and

a message authentication code MAC-A which allows for network to user authentication.

Having received an authentication vector from the home environment, the serving network passes the RAND and AUTN portions of the vector to the user equipment.

With reference to Figure 2, the RAND and AUTN portions are processed by the mobile user equipment. The user equipment processes RAND using a predetermined algorithm f5 which takes as its input also a long term secret key K. This produces the anonymity key AK which can be used to reveal the sequence number SQN.

SQN is then fed into a predetermined algorithm f1 along with RAND and the long term secret key K. This generates XMAC (the expected message authentication code). This is compared with MAC-A and should be equal to MAC-A.

If XMAC is correct, the user equipment then checks that the sequence number SQN which has been generated is greater than SQN_{he}; which is the SQN attached to the last valid

RAND/AUTN combination received from the home environment. This ensures that an authentication vector can only be used once.

If both MAC-A and SQN in the network to user authentication string AUTN pass the above test, then the AUTN is considered valid. The user equipment then processes RAND by applying the long term secret key K via algorithms f2, f3 and f4. This generates the values of RES, IK and CK.

The response (RES) is sent to the serving network which responds with a key set identifier (KSI). The user SIM assigns or tags the generated CK and IK values with the KSI given by the serving network. As described below, the user equipment then passes the KSI to the SN with each request for service.

As noted above, it may be difficult for the home operator to ensure that correct authentication procedures are carried out by the serving network. Described below, are several techniques (which may be selected by sending appropriate instructions via the authentication management field of the authentication vector) which limit the lifetime of the authentication vector thereby requiring the serving network to request a new authentication vector from the home operator.

With reference to Figure 3, once the process shown in Figure 2 is completed, the user equipment may initiate calls via the serving network using the same KSI without requiring

a new vector to be requested by the serving network. Initially, the user equipment sends its current KSI in its first layer three message (this being the message that requests a particular service from the serving network). The serving network checks the KSI received with the message and if it is valid, continues to process the service request. Ciphering and integrity protection are performed using the CK and IK indicated by the KSI.

The user equipment is able to select a KSI value which indicates to the serving network that the user does not have a valid CK or IK at the next service request (for example the next call). Thus, without modifying any of the signalling messages between the home operator and serving network or producing any new procedures for the serving network VLR, it is possible for the user equipment to control the lifetime of the authentication vector.

In the first technique, the authentication management field is used to instruct the user equipment to always issue a KSI which causes a new vector to be requested when service is next requested from the serving network. The effect of this is that an authentication vector is requested for every call made by the user equipment in the serving network. This ensures that full authentication occurs for every call and also means that the home operator is notified of every call made by the user equipment. This means that the home operator has control over the security of the use of the user equipment in the serving network.

In an alternative approach, the user equipment can allow the authentication vector to be used for a predetermined time period, a predetermined number of calls or a predetermined

total call duration (which may span more than one call). These parameters may be monitored by the user equipment using appropriate timers, accumulators and counters. Before requesting service, the mobile user equipment determines whether the authentication vector should still be valid and issues either the KSI given by the serving network (if no new authentication vector is required) or a special KSI which forces the serving network to request a new authentication vector when the next service request is made.

Thus in the first technique above, the AMF may be used to ensure that only one call can be made with the authentication vector containing that AMF. This provides maximum security for the home operator. In the alternative techniques, the risk to the home operator of abuse of the network is reduced because there is choice of a maximum time limit of service, maximum call duration and/or maximum number of calls available with a particular authentication vector.

It will be appreciated that the user equipment may be arranged to implement one, all or a selection of the above techniques, each selected by a particular value of the AMF. Also, the user equipment may implement a combination of the techniques such as forcing a new vector to be requested if a predetermined number of calls have been made or a predetermined time period has expired.

CLAIMS

1. A method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of:

passing an authentication element forming at least part of an authentication vector, from a serving network to mobile user equipment,

deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and

passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

2. A method according to claim 1, wherein the termination message is a predetermined key set identity value.

3. A method according to claim 1 or claim 2, wherein the predetermined field is an authentication management field.

4. A method according to any preceding claim, wherein the said decision is taken based on the total call duration which has accumulated since the authentication

element containing the predetermined field was first received by the mobile user equipment.

5. A method according to any preceding claim, wherein the said decision is taken based on the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment.

6. A method according to any preceding claim, wherein the said decision is taken based on the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment.

7. A SIM for mobile user equipment embodying the method steps of any preceding claim.

8. A method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of:

requesting service from a serving network to which the user equipment is not directly subscribed,

passing the request for service from the serving network to a home operator network to which the user equipment is directly subscribed,

generating an authentication vector in the home operator network which includes an authentication management field,

passing the authentication vector from the home operator network to the serving network,

passing an authentication element forming at least part of the authentication vector from the serving network to the user equipment,

extracting in the user equipment an authentication management field from the authentication element,

generating in response at least to a predetermined value of the authentication management field, a predetermined key set identifier, and

passing the key set identifier to the serving network.

9. A method according to claim 8, including deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a key set identifier which contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

10. A method according to claim 9, wherein the said decision is taken based on the total call duration which has accumulated since the authentication element containing the predetermined field was first received by the mobile user equipment.

11. A method according to claim 9 or claim 10, wherein the said decision is taken based on the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment.

12. A method according to any one of claims 9 to 11, wherein the said decision is taken based on the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment.

13. Mobile user equipment for use in a mobile telecommunications network including means for receiving from a serving network, an authentication element forming at least part of an authentication vector, decision means for deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and means for passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

14. Mobile user equipment according to claim 13, including accumulator means for monitoring the total call duration which has accumulated since the authentication element containing the predetermined field was first received by the mobile user

equipment and providing a value representative of the said total call duration to the decision means.

15. Mobile user equipment according to claim 13 or claim 14, including timer means for measuring the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment and providing a value representative of the said elapsed time to the decision means.

16. Mobile user equipment according to any one of claims 13 to 15, including counter means for counting the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment and providing a value representative of the said total call number to the decision means.

17. A mobile communications network constructed and arranged as described herein with reference to the drawings.

18. Mobile user equipment constructed and arranged as described herein with reference to the drawings.

The Patent Office

14

INVESTOR IN PEOPLE

Application No: GB 9927334.4
Claims searched: 1-16

Examiner: Anita Keogh
Date of search: 23 May 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4L (LDSKA, LDSKF, LDSKX, LEF)

Int Cl (Ed.7): H04Q (7/32, 7/38)

Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2279541 A	(NEC) see figures 8 & 9 and page 2 line 24 to page 4 line 15	1, 8, 13
A	WO 92/02087 A1	(ERICSSON) see page 41, lines 15-33	1, 8, 13
A, E	US 6014558	(THOMAS) see column 1, lines 39-58 and figure 1	
A	US 5471532	(GARDECK et al.) see particularly column 2 line 39 to column 3 line 15	1, 8, 13
A	US 4897875	(POLLARD et al.) see column 6 lines 53-68	1, 8, 13

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.